「ビッグデータ統合利活用のための次世代基盤技術の創出・体系化」
2015 年度採択研究代表者

2018 年度
実績報告書

山名　早人

早稲田大学理工学術院基幹理工学部情報理工学科
教授

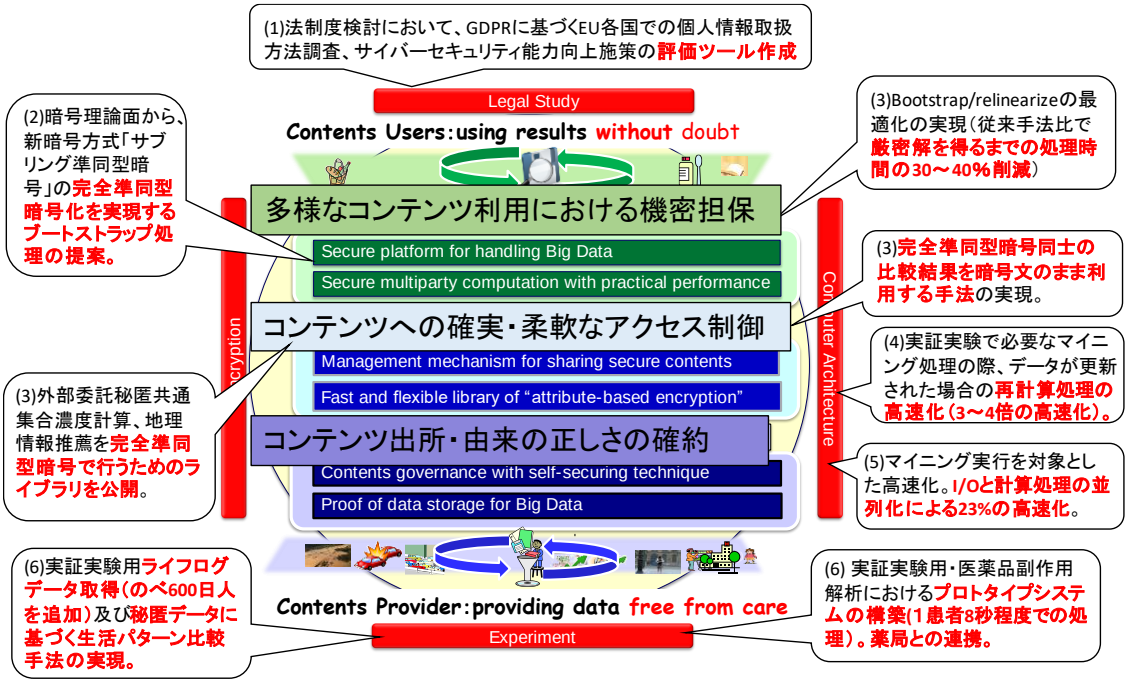
ビッグデータ統合利用のためのセキュアな コンテンツ共有・流通基盤の構築

§1. 研究成果の概要

ビッグデータの利活用推進のためには、コンテンツ提供者が安心してデータを提供でき、コンテンツ利用者が信頼して結果を利用できる基盤が求められる。これに応えるため本研究では、「匿名化」や「通信時の暗号化」から脱却し、コンテンツを常に暗号化した状態で扱うことのできる基盤の構築を目指している。しかし、暗号化した状態で計算を実現するには膨大な時間が必要となるため実用化が困難である。これに対して本研究開発では、暗号理論とコンピュータアーキテクチャの両面で最適化を行うことにより、1,000 倍以上の高速化を行うことを目指している。

4 年目となる平成 30 年度は、完全準同型暗号の実アプリケーションでの応用を推進するために、実証実験として設定している2件のアプリケーション（医薬品副作用解析システム、ライフログデータ取得・解析システム）実現において必要不可欠となる要素技術の研究開発・統合を進めると共に、幅広いアプリケーションに対応するためのライブラリ開発を進め、一部については、GitHub を通じて公開を開始した。また、海外との連携を積極的に推進した。本研究開発では、これまで HElib と呼ばれる完全準同型暗号ライブラリを基礎とし、その高速化と幅広いアプリケーションへの適用を行ってきたが、ニュージャージー工科大学との連携のもと、同大学で新たに開発された PALISADE と呼ばれるライブラリに基づいた各種高速化手法の研究開発を進めた。

本年度の顕著な成果は、図に示す通り、(a)法的検討面から GDPR における個人データの取り扱いの調査、(b)昨年度提案した新暗号プロトコル「サブリング準同型暗号方式」の完全準同型暗号化のためのブートストラップ演算実装、(c)完全準同型暗号同士の比較処理の実現[1]、(d)外部委託秘匿共通集合濃度計算[2]、地理情報推薦処理ライブラリ群の公開、(e)頻出パターンマイニングにおけるデータベース更新時の再計算高速化[3]、(f)I/O 処理チューニングによる 23%の高速化、(g)実証実験アプリケーションの準備である。



【代表的な原著論文】

[1] Yu Ishimaki, Hayato Yamana:″Non-Interactive and Fully Output Expressive Private Comparison,″ Proc. of INDOCRYPT 2018, pp.355-374 (2018.12)

[2] Arisa Tajima, Hiroki Sato, Hayato Yamana:″Outsourced Private Set Intersection Cardinality with Fully Homomorphic Encryption,″ Proc. of the 6th International Conference on Multimedia Computing and Systems (ICMCS2018) (2018.5)

[3] Yuri Yamamoto and Masato Oguchi, ″Distributed Secure Data Mining with Updating Database Using Fully Homomorphic Encryption,″ Proc. of the 13th International Conference on Ubiquitous Information Management and Communication (IMCOM2019), 9-4, January 2019.

§2. 研究実施体制

(1)「山名」グループ

① 研究代表者:山名　早人 （早稲田大学理工学術院基幹理工学部情報理工学科　教授）

② 研究項目

・暗号ライブラリ構築(コンピュータアーキテクチャ面からの高速化)

・クラウドプラットフォーム構築

(2)「後藤」グループ

① 主たる共同研究者:後藤　厚宏 （情報セキュリティ大学院大学情報セキュリティ研究科　教授）

② 研究項目

・法的検討・ガイドライン策定

・暗号ライブラリ構築(暗号理論面からの高速化)

(3)「小口」グループ

① 主たる共同研究者:小口　正人 （お茶の水女子大学基幹研究院　教授）

② 研究項目

・クラウドプラットフォーム構築

(4)「山口」グループ

① 主たる共同研究者:山口　実靖 （工学院大学情報学部情報通信工学科　准教授）

② 研究項目

・暗号ライブラリ構築(I/O 面からの高速化)

(5)「新谷」グループ

① 主たる共同研究者:新谷　隆彦 （電気通信大学大学院情報理工学研究科　准教授）

② 研究項目

・実証実験(ライフログデータ取得・解析システム構築)

(6)「野口」グループ

① 主たる共同研究者:野口　保 （明治薬科大学薬学部薬学教育研究センター数理科学部門教授）

② 研究項目

・実証実験(医薬品副作用解析システム構築)